Iowa Department of Administrative Services

Chester J. Culver, Governor
Patty Judge, Lt. Governor

Mollie K. Anderson, Director

STATE OF IOWA SHARED AUTHENTICATION STANDARD

Purpose

This Standard establishes shared authentication requirements for State of Iowa agencies. Shared authentication is a pre-requisite for integration of State computing resources and sharing of data.

Overview

The State of Iowa maintains a variety of data in its computer systems, including confidential and sensitive customer information. Protection of customer data from unauthorized access requires that adequate authentication procedures be in place.

Under the direction of the State's Technology Governance Board (TGB), a Working Group was formed to create a recommended statewide standard for shared authentication. The Standard will allow the State to standardize the types of credentials issued to users, and to standardize the process by which credentials are granted. Centralizing the repository for credentials will also allow users to apply their existing credentials access various State systems, making for easier deployment of new systems.

Creating a “menu” of authentication options will allow business owners to make decisions on the level of control appropriate for authenticating users to their applications. Stronger controls may require additional steps in authentication, but reduce risk of unauthorized access. The menu will allow State program managers and system owners to easily choose the authentication level that provides the best balance of risk, cost and convenience.

Scope

Who must comply? Any RFP, procurement or system development review made by the TGB may include this Standard as criteria for approval. All State agencies that fall under TGB governance are affected by this Standard.

What is included? This Standard covers authentication by end-users, be they State employees, local government, citizens or business entities, to State-managed computing resources, such as e-mail, desktop applications, web sites and web services. It also includes authentications made between systems on behalf of an end-user, especially when the identity or authorization of the “calling” system’s end user affects the processing done by the “called” system.

What is not included? Transport and device-level security mechanisms (such as IP or MAC filtering), encryption, penetration testing or other application security measures are not included. Network authentication (such as Windows accounts) are not included, with the exception that such accounts should be shared through trusts wherever possible. System integration tasks where no specific user is involved (such as automated batch feeds between computers) are not included.

How is it enforced? The TGB has sole authority to enforce the Standard by approval or denial of an RFP, procurement, or system development request.

Variances and Exceptions

Agencies may request a variance from the Standard if one of the following criteria is met.

- The application is subject to federal authentication requirements that conflict with this Standard,

or

- The cost of meeting the standard is prohibitive and an alternate authentication method is sufficient in preventing unauthorized access,

or

- The security requirements of the application are greater than those currently provided by the Standard and existing infrastructure. In that case, every effort should be taken to make the additional security mechanism(s) part of the shared infrastructure for re-use by others.

Requests for variances will be submitted to and evaluated by the TGB (and their delegates), using existing standards as the basis for assessment.

Authentication Standard

Centralized Account Repository

State systems that are covered by this Standard ("Systems", herein) will store user credentials in a centralized repository. State and non-State accounts will be made available to any application that uses the repository. Each account should be assigned to a single person, not a group or entity, to maintain the integrity of each account and the secrecy of its password.

The repository will provide the following basic operations:

- Encryption and comparison of the shared secret (password)
- Aging of the password and enforcement of password changing rules
- Flexible password complexity rules
- Open standards for accessing account information (e.g., ODBC, LDAP, etc.)

The repository will integrate with existing State accounts (AD Domains) wherever possible to provide use of those accounts as credentials.

Multi-Factor Authentication

Use of multi-factor authentication provides a higher level of protection for Systems. Using multiple factors can also increase the cost and difficulty associated with using a System. Agencies should balance the risk of unauthorized access to their data against the cost of implementing an authentication method(s). In addition, certain types of data carry specific requirements based on industry, Federal or State standards. Examples of multi-factor authentication bundles include:

- User ID & Password + Secret Questions
- User ID & Password + Certificate
- User ID & Password + Token Generator
- User ID & Password + Token Generator + Certificate

Standard Credential Types

This section outlines the standard credential types for Shared Authentication. After a brief description of the credential type, the pros and cons of that type are listed. Each credential type includes a color-coded table that identifies *relative* values for the following:

- **Cost**: The cost to the State for implementing a centralized credential of this type. Also refers to the per-unit provisioning cost.
- **Strength**: The difficulty with which the credential can be obtained illicitly, stolen, or forged.
- **Factor**: What kind of credential: Something the user *knows*, *has*, or *is*.

1. User ID and Password

Cost: LOW	Strength: LOW	Factor: KNOW

A user-selected identifier with the suffix @IowaID for external users and *.iowa.gov or *.state.ia.us for State users, and a password that follows the existing State (or Agency) Information Security policy for complexity, aging and history.

The default value for a given user ID will be firstname.lastname@IowaID, but it must be unique and may be edited at registration-time. User IDs will not be re-usable: that is, if an account is deactivated for some reason, no one else will be able to use that same ID, ever. Inactive User IDs will be kept in the centralized repository for this purpose.

By default, passwords for self-registered Accounts will not expire. User's participating in an in-person verification process will be marked as "in-person verified". The expiration flag will be set for "in-person verified users", and the Account's password will be governed according to the State standard for password aging. Password complexity and history requirements will be the same in either case.

Pros:
- Portable
- Nothing to install
- Familiar to users

Cons:
- Difficult to detect theft
- Difficult for users to maintain secure passwords

2. Secret Questions

Cost: LOW	Strength: LOW	Factor: KNOW

User-selected questions and answers. The answers are stored like passwords, encrypted in the repository. Two questions are selected from a list of common examples, and the third question is entered by the user. The user must enter each answer twice, since the fields are masked and cannot be read (like password fields).

Pros:
- Portable
- Nothing to install
- Somewhat familiar to users

Cons:
- Difficult to detect theft
- Users can forget their answers

3. Certificate

Cost: MED	Strength: LOW	Factor: HAVE

A State-issued data file that contains encrypted data. Certificates can be installed to a web browser and submitted automatically with web page requests to validate the requestor. A certificate can be proven to have been issued by the State or not.

Pros:
- Semi-portable: Can be installed to multiple computers (work, home, etc.)
- Automatically used when installed

Cons:
- Requires installation by the user
- Difficult to detect theft
- Does NOT prove who the user is, just that they HAVE the certificate

4. Token Generator

Cost: MED	Strength: MED	Factor: HAVE

A random-number generator that creates a new password every few seconds.

Pros:
- Portable
- Nothing to install
- Prevents “replay” attacks (see Definitions, above)
- Provides non-repudiation (see Definitions, above)

Cons:
- Requires a physical token
- Tokens are expensive ($50-$100)

Definitions

Authentication: The process of establishing confidence in user identities.

Certificate: A digital representation which minimally:

- Identifies the certification authority issuing it,
- Names or identifies its subscriber,
- Contains the subscriber's public key,
- Identifies its operational period, and
- Is digitally signed by the certification authority issuing it.

Certification Authority: A trusted entity that issues and revokes public key certificates.

CISO: Chief Information Security Officer. Responsible for overall Enterprise information security.

Confidential Data: Data protected by state or federal law.

Credential: An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.

Non-repudiation: Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

Password: A secret that a user possesses and uses to authenticate his or her identity. Passwords are typically character strings.

Portability: The characteristic of an authentication method, which allows a user to authenticate from more than one computer.

Replay Attack: A breach of security in which information is stored without authorization and then retransmitted to trick the receiver into unauthorized operations such as false identification/authentication or a duplicate transaction.

Sensitive Data: Data not explicitly protected by law, but exposure of which could result in negative impact to government services, state government partners or citizens.

Token: Something that a user possess and controls (typically a key or password) used to authenticate the user's identity.

Token Generator: A device that creates a one-time token. The token is generally a value that could not be guessed easily, and changes over time (e.g., every 30 seconds). The token generated is then compared to the value on a server that uses the same algorithm and has previously been synchronized with the token.